## REMARKS

This application has been carefully considered in connection with the Examiner's Action. Reconsideration and allowance are respectfully requested in view of the foregoing.

### I.      Summary of Amendment

The Specification has been amended to update the status of the parent of the present application, remove legal terminology inadvertently included in/update the "Summary of the Invention" to reflect the removal of certain ambiguities from original Claim 38, correct a minor typographical error, add inadvertently omitted reference numerals, correct minor grammatical errors and improve the overall readability of the amended passages. In amending the Specification, no new matter has been added. Accordingly, the Applicants respectfully request entry of the foregoing amendment to the Specification.

Claims 1, 20, 32 and 43 have been amended to ensure that all elements thereof enjoy proper antecedent basis. Claims 19 and 20 have been amended to correct minor informalities therein. Finally, Claim 38 has been amended to remove and/or correct the use of certain phraseology contributing to a lack of clarity therein. It is submitted that none of the foregoing amendments to the claims represent a substantive amendment thereto. Accordingly, any subsequent rejection of the claims of this application based upon art not previously applied thereagainst cannot properly be made final.

### II.     Applicants' Invention

In certain aspects thereof, the Applicants have invented and claim a security system which includes a security gateway and a security system server. The security gateway is operable to detect an alarm condition and to record an Alarm Video. The security system server is operatively

19

coupled to the security gateway through first and second networks. Importantly, the security gateway transfers different types of information to the security system server over the respective ones of the first and second networks. More specifically, the security gateway is configured to notify the security system server of the alarm condition and to transfer the Alarm Video to the security system server over the first network. In contrast, over the second network, the security gateway is only configured to notify the security system server of the alarm condition.

By configuring the security system in this manner, a high degree of redundancy is built into the security system. More specifically, in the event that the first network over which the notification of the alarm condition and the Alarm video are normally transferred fails, the security system server will still be able to receive the notification of the alarm condition over the second network. Thus, while less information will be provided over the second network, in the event that the first network fails, the security system server will still be notified of an alarm condition and may initiate appropriate action in response thereto. Conversely, as all of the information normally transferred over the second network is also transferred over the first network, the failure of the second network will not affect the information received by the security system server. Thus, once again, the security system server may initiate appropriate action in response to a notification of an alarm condition and receipt of an alarm video. In this manner, the security system server will be capable of initiating appropriate action in spite of the failure of either one of the first and second networks.

**III.    The Rejection of Claims 1, 2, 5 and 13 as anticipated by U.S. 6,385.772 to Courtney**

Claims 1, 2, 5 and 13 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,385,772 to Courtney. In response, the Applicants respectfully traverse the Examiner's rejection and instead submit that Claims 1, 2, 5 and 13 are neither taught nor suggested by

20

Courtney. In rejecting these claims, the Examiner characterizes Courtney as disclosing a system in which computer 24 is coupled to cellular base station 36 by first and second networks—the first being Internet 38 and the second being telephone 41. It is noted, however, while Courtney does indeed disclose a pair of network connections between the computer 24 and the cellular base station 36, the network connections are not used in a redundant manner, i.e., a manner by which an alarm notification will be transmitted from the computer 24 and the cellular base station 36 by one of the two network connections in spite of the failure of the other of the two network connections.

The Examiner cites col. 6, line 54 through col. 7, line 8 of Courtney as disclosing the transfer of the notification of the alarm condition over the first network and col. 6, lines 38 through 53 as disclosing the transfer of the notification of the alarm condition over the second network. The Applicants respectfully disagree and instead submit that the cited passages merely disclose two different methods by which the occurrence of an event of interest may be determined and the use of a <u>single</u> network to transfer either: (a) a notification that an event of interest has potentially occurred; or (b) notification that an event of interest has actually occurred, In this regard, the Applicants respectfully note that the passage at col. 6, lines 38 through 53 discloses a process in which, upon detection of a heat source, the computer 24 issues a notification "<u>through the telephone line 41</u>." Upon receipt of the notification, the operator would access the computer 24 over Internet 38 to determine if an event of interest has occurred in the monitored area. Thus, the foregoing passage discloses a system in which the computer 24 issues a notification of a potential event of interest over a first network, specifically, telephone line 41, and the operator subsequently accesses the computer 24 over a second network, specifically, Internet 38, to determine whether an event of interest has actually occurred.

21

In contrast with the foregoing, the passage extending from col. 6, line 54 through col. 7, line 8 teaches the determination of the occurrence of an event of interest by the computer 24. Once the computer 24 has determined that an event of interest has occurred, however, the computer 24 again uses the telephone line 41 to issue a notification to the operator. In this regard, the Examiner's attention is respectfully directed to col. 7, lines 13 through 15 which states, in relevant part, that "[t]his condition can be used to trigger a telephone call from the computer 24 to the portable unit 46."

By transmitting both notifications over the telephone line, the system disclosed in Courtney is not equipped with the redundant notification capability disclosed and claimed by Applicants. More specifically, in Courtney, failure of the telephone line 41 will prevent any type of information —whether notification of a potential occurrence of an event of interest or notification of an actual occurrence of an event of interest—to reach the operator. In contrast, Applicants' invention provides two paths for a notification to be transmitted. Thus, in the event that one network fails, a notification will still be received over the other network.

For the foregoing reasons, the Applicants respectfully submit that Claims 1, 2, 5 and 13 are neither taught nor suggested by Courtney. Accordingly, the Applicants respectfully request the reconsideration and withdrawal of the rejection of Claims 1, 2, 5 and 13 under 35 U.S.C. § 102(e) as anticipated by Courtney.

**IV.    The Rejection of Claims 1-46 as anticipated by U.S. 2002/0005894 to Foodman**

Claims 1-46 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication No. 2002/0005894 to Foodman. In response, the Applicants respectfully traverse the Examiner's rejection and instead submit that Claims 1-46 are neither taught nor suggested by

Foodman. In rejecting Claims 1-46 as anticipated by Foodman, it appears that the Examiner uses two separate analyses of the reference, the first for Claims 1-37 and the second for Claims 38-46. Accordingly, the Applicant shall address these two analyses separately.

### A. The Rejection of Claims 1-37

In rejecting Claims 1-37, the Examiner characterizes Foodman as disclosing a security system in which security system 311 is operatively coupled to website 321 through both a first network and through a second network. The Examiner further characterizes Foodman as disclosing the transfer of a notification of an alarm condition and an alarm video over the first network and the transfer of the notification of the alarm condition over the second network. The Applicants respectfully disagree with the foregoing characterization of Foodman and instead submit that, when properly characterized, Foodman neither teaches nor suggests Applicants' invention as set forth in Claims 1-37.

More specifically, the Applicants have carefully reviewed the Foodman reference and have failed to find any teaching or suggestion of first and second network connections between the security system 311 and the website 321. While Foodman does identify a number of different types of possible network connections between the security system 311 and the website 321, a careful reading of the reference reveals that Foodman teaches only the use of a single network connection between the security system 311 and the website 321 and discloses a number of different types of possible network connections as alternate ways to accomplish the single network connection contemplated thereby. In this regard, the Examiner's attention is respectfully directed to FIGs. 3B-1 and 3B-2 which disclose a single link between the security system 311 and the website 321, specifically, the link extending from video/audio encoder 317 to website 321 through transmitter

23

319 and communication link 320. In support of the foregoing characterization of FIGs. 3B-1 and

3B-2, the Examiner's attention is respectfully directed to paragraph 15 of Foodman which provides,

in relevant part, that "[c]ommunications to the website is by one of the following internet compliant

communications means: standard phone line, broad band bi-directional cable connection, digital

subscriber line ('DSL'), wireless phone service **or** any other internet compliant communication

format." Foodman, paragraph 15, lines 1-5 (emphasis added by Applicants). In contrast with

Foodman, the Applicants have disclosed and claimed a system in which the security gateway is

coupled to the security system server by two separate and discrete networks. For example,

Applicants' Claim 1 specifically recites at lines 7-8 that the security gateway is coupled to the

security system server through a first network and further recites at lines 12-13 that the security

gateway is coupled to the security system server through a second network.

Nor may the Examiner properly extend the teachings of Foodman to render the claimed

invention obvious. Specifically, even if the Examiner chose to assert Foodman's teaching of

multiple types of network connections clearly disclosed in the context of alternate methods of

coupling the video/audio encoder 317 to the website 321 as suggesting multiple network

connections between the two, nowhere does Foodman teach or even remotely suggest the transport

of different types of information over the different network connections. In contrast, Applicants'

invention is directed to a system in which the security gateway is coupled to the security system

server by first and second networks and in which the security gateway transfers different types of

information to the security system server over different ones of the first and second networks. For

example, Applicants' Claim 1 specifically recites at lines 8-10 that the security gateway both

notifies the security system server of the alarm condition and transfers the alarm video to the

security system server over the first network and further recites at lines 13-15 that the security

gateway merely notifies the security system server of the alarm condition over the second network.

## B.     The Rejection of Claims 38-46

In rejecting Claims 38-46 as anticipated by Foodman, the Examiner characterized Foodman

as disclosing a security system which includes a data center, a user information database comprising

account information and a monitoring client. However, by identifying the "data center" as being

comprised of a pair of disparate elements of the Foodman system, specifically, website 321 and

central monitor 31 and by further identifying the central monitor 31 as serving as both the data

center and the monitoring client for the Foodman system, it appears that the Examiner has failed to

fully appreciate Applicants' security system as defined by Claims 38-46 and how the claimed

security system is distinguishable over the cited art.

For example, Claim 38 is directed to a security system which includes four discrete

elements—a security gateway, a security system server, a data center and a monitoring client—in

which specific functions and/or information are uniquely distributed amongst the various discrete

elements of the security system. Of these elements, the data center includes a database in which

user data is maintained. The security system server, which receives a notification of an alarm

condition and an alarm video from the security gateway, associates at least a portion of the user data

with the alarm video. The security system server then transmits the notification of the alarm

condition, the alarm video and the associated user data to the monitoring client. There, at least a

portion of the alarm video and the associated user data is displayed.

By distributing functions and/or information in the foregoing manner, the Applicants have

disclosed and claim a security system neither taught nor suggested by Foodman. More specifically,

25

in Foodman, the website 321 receives an account code 403-1 from system 311 which identifies the particular premises for which an alarm condition has been detected. The website 317 then "uses the provided account code to verify within its database of existing customers that the connected premises are an active account" and to "determine the proper central monitor 31 in its database that services the account 415." *See* Foodman, paragraph 39, lines 10-12 and paragraph 40, lines 2-4. The website establishes a temporary web page and notifies the central monitor 31 and the owner 330 of the event. The central monitor 31 and the owner 330 are then "able to access the temporary web page 407, 422" established for the event. *See* Foodman, paragraph 40, lines 13-14.

In contrast with the security system disclosed and claimed by the Applicants, Foodman neither teaches nor suggests a security system in which a first discrete element retrieves user data from a second discrete element, associates the retrieved user data with an alarm video received from a third discrete element and transmits the alarm video and the associated user data to a fourth discrete element. By uniquely distributing functions and/or information in this manner, Applicants' security system advantageously distinguishes itself over the system disclosed by Foodman. More specifically, Foodman uses information to determine whether an account is active and which central monitor is assigned to a premises. Foodman neither teaches nor suggest the retrieval of information for any purpose other than identification. While useful to the website 321 which retrieved the information, the retrieved information has no value to the central monitor 31 and/or owner 310. Accordingly, the retrieved information is never made available for access by the central monitor 31 and/or owner 310.

The system disclosed and claimed by the Applicants, on the other hand, retrieves information useful to the monitoring client. Accordingly, upon retrieval of the information from the

26

data center, the security system server associates the retrieved information with the alarm video and

transmits the two to the monitoring client. In this manner, the monitoring client is better equipped

to resolve a potential alarm condition than if it was provided with the alarm video alone.

Furthermore, by maintaining and distributing user information in this manner, the monitoring client

will only receive that portion of the user data selected by the security system server as relevant to

the alarm condition. Unused information will not be transmitted. As a result, the confidentiality of

user information which is not necessary for resolution of a potential alarm condition by the

monitoring client will remain confidential.

For the foregoing reasons, the Applicants respectfully submit that Claims 1-46 are neither

taught nor suggested by Foodman. Accordingly, the Applicants respectfully request the

reconsideration and withdrawal of the rejection of Claims 1-46 under 35 U.S.C. § 102(e) as

anticipated by Foodman.

V.      **The Rejection of Claims 38-46 as anticipated by U.S. 6,400,265 to Saylor et al.**

Claims 38-46 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent

No. 6,400,265 to Saylor et al. In response, the Applicants respectfully traverse the Examiner's

rejection and instead submit that Claims 38-46 are neither taught nor suggested by Saylor et al.

More specifically, similar to Foodman, Saylor et al. fails to teach or suggest a security system in

which selected functions and/or information are distributed amongst plural elements. As previously

set forth, Applicants' invention, as defined by Claim 38, is directed to a security system which

includes four discrete elements—a security gateway, a security system server, a data center and a

monitoring client—in which specific functions and/or information are uniquely distributed amongst

the various discrete elements of the security system. Of these elements, the data center includes a

database in which user data is maintained. The security system server, which receives a notification of an alarm condition and an alarm video from the security gateway, associates at least a portion of the user data with the alarm video. The security system server then transmits the notification of the alarm condition, the alarm video and the associated user data to the monitoring client. There, at least a portion of the alarm video and the associated user data is displayed.

In contrast, Saylor et al. discloses a highly centralized system which lacks the distributed functionality of Applicants security system. In Saylor et al., the central security server 130 receives information related to potential alarm condition, accesses information maintained in databases, resolves the potential alarm condition and issues notifications of the resolved alarm condition to identified individuals.

In contrast with the security system disclosed and claimed by the Applicants, <u>Saylor et al.</u> <u>neither teaches nor suggests a security system in which a first discrete element retrieves user data</u> <u>from a second discrete element, associates the retrieved user data with an alarm video received from</u> <u>a third discrete element and transmits the alarm video and associated user data to a fourth discrete</u> <u>element</u>. By uniquely distributing functions and/or information in this manner, Applicants' security system advantageously distinguishes itself over the system disclosed by Saylor et al. More specifically, in Saylor et al., nearly all of the functionality and information of the security system resides in the central security server 130. In contrast, the Applicants have disclosed and claimed a security system which distributes that functionality amongst plural elements, certain ones of which have no corresponding elements in the security system disclosed by Saylor et al. For example, nowhere does Saylor et al. teach or suggest a discrete monitoring client which resolves a potential alarm condition using the alarm video and associated user information transmitted thereto by the

28

security system server. Instead, Saylor et al. teaches that the potential alarm condition is resolved by the central security server 130 and, subsequent to resolution thereof, user 160 is simply notified of the resolved alarm condition. Furthermore, the Applicants' security system is configured such that user data maintained in the data center is accessed only by the security system server. As a result, the monitoring client will only receive that portion of the user data selected by the security system server as being relevant to the alarm condition. Unused information will not be transmitted. As a result, the confidentiality of user information which is not necessary for resolution of a potential alarm condition by the monitoring client will remain confidential. In contrast, the central security server disclosed in Saylor et al. will have access to confidential information irrelevant to the resolution of an alarm condition.

For the foregoing reasons, the Applicants respectfully submit that Claims 38-46 are neither taught nor suggested by Saylor et al. Accordingly, the Applicants respectfully request the reconsideration and withdrawal of the rejection of Claims 38-46 under 35 U.S.C. § 102(e) as anticipated by Saylor et al.

## VI.    The Provisional Obviousness-Type Double Patenting Rejection of Claims 38 and 43

Claims 38 and 43 stand provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over Claims 1 and 17 of copending Application No. 09/969,521. To overcome this rejection, the Applicants submit herewith a Terminal Disclaimer in compliance with 37 CFR 1.321(c). Accordingly, the Applicants respectfully request the reconsideration and withdrawal of the provisional rejection of Claims 38 and 43.

## VII. Concluding Remarks

For the reasons set forth herein, the Applicants respectfully request the reconsideration and withdrawal of the various rejections of Claims 1-46 and the allowance of the claims. As the Examiner's Action was mailed on September 2, 2004, a Request for Extension of Time to January 3, 2005 and the fee associated therewith is attached to this Response. The Commissioner is authorized to charge any additional fees connected with this communication or credit any overpayment to Deposit Account No. 50-1515.

While the foregoing amendment and associated remarks are believed to clearly establish the patentability of Claims 1-46, if a telephonic interview with the attorney of record will expedite the issuance of a Notice of Allowability, the Examiner is invited to call the undersigned.

Respectfully submitted,

Date: January 3, 2005

Michael S. Bush
Reg. No. 31,745
Conley Rose, P.C
5700 Granite Parkway, Suite 330
Plano, Texas 75024
(972) 731-2288
ATTORNEY FOR APPLICANTS

23532.01/4017.03001